In the claims:

1. (currently amended) A communication system comprising:

a rendezvous point device that forwards multicast communication messages to members of a shared tree and is a root of the shared tree;

a designated device in communication with the rendezvous point device via a number of intermediate devices; and

a host device in communication with the designated device, wherein to join the shared tree:

the host device forwards an authentication key, uniquely generated by a key server for the host device, to the designated device;

the host device sends a join request to the designated device using a predetermined multicast group management protocol in order to join the shared tree for receiving the multicast communication messages forwarded by the rendezvous point device, the join request including the authentication key;

the designated device receives the join request and forwards to the rendezvous point device via the number of intermediate devices an encoded join request, wherein the encoded join request comprises a tag field computed using a keyed hashed function and the authentication key ~~and a nonce field comprising a number for preventing playback attack~~;

the rendezvous point device receives the encoded join request and authenticates the encoded join message ~~using~~ by comparing the authentication key received in the tag against a stored authentication key associated with the host device; wherein

the host device is prevented from receiving the multicast communication messages forwarded by the rendezvous point device, if the rendezvous point device determines that the encoded join message is not authentic.

2. (cancelled)

3. (previously presented) The communication system of claim 1, wherein the key server provides the authentication key to both the host device and the rendezvous point device using a secure key distribution mechanism.

4. (cancelled)

5. (previously presented) The communication system of claim 5, wherein the host device sends the authentication key to the designated device in the join request.

6. (original) The communication system of claim 5, wherein the predetermined multicast group management protocol is an extended Internet Group Management Protocol (IGMP) including means for including the authentication key in the join request.

7. (original) The communication system of claim 1, wherein the designated device joins the shared tree on behalf of the host device.

8. (original) The communication system of claim 7, wherein the designated device establishes appropriate multicast routes for forwarding multicast communication messages to the host.

9. (original) The communication system of claim 1, wherein each intermediate device receives the encoded join request and forwards the encoded join request toward the rendezvous point device.

10. (original) The communication system of claim 9, wherein each intermediate device that is not already joined to the shared tree joins the shared tree on behalf of the host device and establishes appropriate multicast routes for forwarding multicast communication messages toward the host device upon receiving the encoded join request.

11. (original) The communication system of claim 9, wherein each intermediate device that is already joined to the shared tree waits for an explicit acknowledgment message from the

rendezvous point device and establishes appropriate multicast routes for forwarding multicast communication messages toward the host device only upon receiving the explicit acknowledgment message from the rendezvous point device.

12. (original) The communication system of claim 1, wherein the rendezvous point device sends an explicit acknowledgment message toward the host device upon determining that the encoded join request is authentic.

13. (canceled).

14. (canceled)

15. (canceled)

16. (canceled).

17. (canceled)

18. (currently amended) A method comprising:

obtaining an authentication key uniquely associated with a host device from a key server along with a group membership key following authentication of the host device by the key server; and

sending a join request to a designated device using a predetermined multicast group management protocol, the join request including the authentication key for use by the designated device for encoding the join message prior to forwarding of the join message to a rendezvous point wherein the join message is encoded by inserting a tag field computed using a keyed hash function and the authentication key ~~and a nonce field comprising a number for preventing playback attack~~.

19. (original) The method of claim 18, wherein the predetermined multicast group management protocol is an extended Internet Group Management Protocol (IGMP) including means for including the authentication key in the join request.

20. (currently amended) An apparatus comprising:

receiving logic operably coupled to receive an authentication key uniquely generated for the apparatus and to receive a group membership key from a key server following authentication of the host device by the key server; and

joining logic operably coupled to send a join request to a designated device using a predetermined multicast group management protocol, the join request including the authentication key for use by the designated device for encoding the join message prior to forwarding of the join message to a rendezvous point, to enable authentication of the join message at the rendezvous point by comparison of the ~~using the~~ authentication key associated with the host device against a stored key associated with the apparatus.

21. (original) The apparatus of claim 20, wherein the predetermined multicast group management protocol is an extended Internet Group Management Protocol (IGMP) including means for including the authentication key in the join request.

22. (canceled)

23. (canceled)

24. (canceled)

25. (canceled)

26. (currently amended) A method of authentication a host device for access to a shared tree comprising:

receiving a join request from a host device;

generating an encoded join request using an authentication key uniquely associated with the host device, wherein the encoded join request comprises a tag field computed using a keyed hash function and the authentication key ~~and a nonce field comprising a number for preventing playback attack~~, the authentication key being received together with a group key by the host device following authentication of the host device by a key server and forwarded in the join request from the host device; and

sending the encoded join request toward a rendezvous point device at the root of the shared tree to enable authentication of the join message at the rendezvous by comparing ~~point using~~ the authentication key uniquely associated with the host device against a stored authentication key associated with the host device at the rendezvous point.

27. (original) The method of claim 26, wherein the join request includes the authentication key.

28. (original) The method of claim 26, further comprising:

joining a shared tree on behalf of the host device and establishing appropriate multicast routes for forwarding multicast communication messages to the host device.

29. (currently amended) An apparatus for securing a shared tree comprising:

receiving logic operably coupled to receive a join request from a host device;

encoding logic operably coupled to generate an encoded join request using an authentication key uniquely associated with the host device, wherein the encoded join request comprises a tag field computed using a keyed hash function and the authentication key ~~and a nonce field comprising a number for preventing playback attack~~, the authentication key being received by the host device following authentication of the host device by a key server and forwarded in the join request from the host device; and

sending logic operably coupled to send the encoded join request toward a rendezvous point device at the root of the shared tree to enable authentication of the join message at the rendezvous point by comparing ~~using~~ the authentication key associated with the

host device against a stored authentication key associated with the host at the rendezvous point.

.

30. (original) The apparatus of claim 29, wherein the join request includes the authentication key.

31. (original) The apparatus of claim 29, further comprising:

joining logic operably coupled to join a shared tree on behalf of the host device; and

routing logic operably coupled to establish appropriate multicast routes for forwarding multicast communication messages to the host device.

32. (currently amended) A computer readable medium having embodied therein a computer program for controlling a computer system, the computer program comprising:

receiving logic programmed to receive a join request from a host device;

encoding logic programmed to generate an encoded join request using an authentication key uniquely associated with the host device, [[,]]wherein the encoded join request comprises a tag field computed using a keyed hash function and the authentication key ~~and a nonce field comprising a number for preventing playback attack~~, the authentication key being received by the host device together with a group key following authentication of the host device by a key server and forwarded in the join request from the host device; and

sending logic programmed to send the encoded join request toward a rendezvous point device to enable authentication of the join message at the rendezvous point by comparing ~~using~~ the authentication key associated with the host device against a stored key associated with the host device at the rendezvous point.

.

33. (original) The computer readable medium of claim 32, wherein the join request includes the authentication key.

34. (original) The computer readable medium of claim 32, further comprising:

joining logic operably coupled to join a shared tree on behalf of the host device; and

routing logic operably coupled to establish appropriate multicast routes for forwarding multicast communication messages to the host device.

35. (original) The computer readable medium of claim 32, wherein the computer readable medium is a computer storage medium.

36. (original) The computer readable medium of claim 32, wherein the computer readable medium is a computer communication medium.

37. (canceled)

38. (canceled)

39. (canceled)

40. (canceled)

41. (canceled)

42. (canceled)

43. (canceled)

44. (canceled)

45. (canceled).

46. (canceled).

47. (canceled).

48. (currently amended) A method comprising:

receiving, from a designated routing device coupled to a host, an encoded join request for the host device, the encoded join request being encoded by the designated routing device using an authentication key uniquely associated with the host, wherein the encoded join request comprises a tag field computed using a keyed hash function and the authentication key ~~and a nonce field comprising a number for preventing playback attack~~, the authentication key being received by the host device following authentication of the host device by a key server and forwarded in a join request forwarded from host device to the designated routing device;

authenticating the encoded join request using the host device authentication key to determine whether or not the encoded join request is authentic by comparing the authentication key against a stored authentication key uniquely associated with the host; and

establishing appropriate multicast routes for forwarding multicast communication messages to the host device if and only if the encoded join request is determined to be authentic.

49. (currently amended) The method of claim 48, wherein authenticating the encoded join request

comprises:

maintaining a number of authentication keys uniquely associated with a corresponding number of host devices;

determining the host device for the encoded join request; and searching a storage device for an authentication key uniquely associated with the host device.

50. (original) The method of claim 49, wherein authenticating the encoded join request further comprises:

failing to find an authentication key associated with the host device; and

determining that the encoded join request is not authentic.

51. (original) The method of claim 49, wherein authenticating the encoded join request further comprises:

finding an authentication key associated with the host device; and authenticating the encoded join request using the authentication key associated with the host device.

52. (original) The method of claim 48, further comprising:

sending an explicit acknowledgment toward the host device if and only if the encoded join request is determined to be authentic.

53. (currently amended) An apparatus comprising:

receiving logic operably coupled to receive an encoded join request for a host device, the encoded join request being encoded and forwarded by a designated routing device coupled to the host device using an authentication key uniquely associated with the host device, wherein the encoded join request comprises a tag field computed using a keyed hash function and the authentication key ~~and a nonce field comprising a number for preventing playback attack~~, the authentication key being received by the host device following authentication of the host device by a key server and forwarded in a join request forwarded from host device to the designated routing device;

authenticating logic operably coupled to authenticate the encoded join request by comparing ~~using~~ the host device authentication key to a stored authentication key associated with the host device to determine whether or not the encoded join request is authentic; and

routing logic operably coupled to establish appropriate multicast routes for forwarding multicast communication messages to the host device if and only if the encoded join request is determined to be authentic.

54. (original) The apparatus of claim 53, wherein the authenticating logic is operably coupled to maintain a number of authentication keys, determine the host device for the encoded join request, and search for an authentication key associated with the host device.

55. (original) The apparatus of claim 54, wherein the authenticating logic is operably coupled to determine that the encoded join request is not authentic if the authenticating logic fails to find an authentication key associated with the host device.

56. (original) The apparatus of claim 54, wherein the authenticating logic is operably coupled to authenticate the encoded join request using an authentication key associated with the host device if the authenticating logic finds the authentication key associated with the host device.

57. (original) The apparatus of claim 53, further comprising:

acknowledgment logic operably coupled to send an explicit acknowledgment toward the host device if and only if the encoded join request is determined to be authentic.

58. (currently amended) A computer readable medium having embodied therein a computer program for controlling a computer system, the computer program comprising:

receiving logic programmed to receive an encoded join request for a host device ~~receiving logic operably coupled to receive an encoded join request for a host device,~~ the encoded join request being encoded and forwarded by a designated routing device coupled to the host device using an authentication key uniquely associated with the host device, the authentication key being received by the host device together with a group key following authentication of the host device by a key server and forwarded in a join request forwarded from host device to the designated routing device;

authenticating logic programmed to authenticate the encoded join request by comparing the ~~using~~ the host device authentication key against a stored authentication key associated with the host device to determine whether or not the encoded join request is authentic; and

routing logic programmed to establish appropriate multicast routes for forwarding multicast communication messages to the host device if and only if the encoded join request is determined to be authentic.

59. (original) The computer readable medium of claim 58, wherein the authenticating logic is programmed to maintain a number of authentication keys, determine the host device for the encoded join request, and search for an authentication key associated with the host device.

60. (original) The computer readable medium of claim 59, wherein the authenticating logic is programmed to determine that the encoded join request is not authentic if the authenticating logic fails to find an authentication key associated with the host device.

61. (original) The computer readable medium of claim 59, wherein the authenticating logic is programmed to authenticate the encoded join request using an authentication key associated with the host device if the authenticating logic finds the authentication key associated with the host device.

62. (original) The computer readable medium of claim 58, further comprising:

acknowledgment logic programmed to send an explicit acknowledgment toward the host device if and only if the encoded join request is determined to be authentic.

63. (original) The computer readable medium of claim 58, wherein the computer readable medium is a computer storage medium.

64. (original) The computer readable medium of claim 58, wherein the computer readable medium is a computer communication medium.

65. (currently amended) In a communication system having a host device, a designated device, and a rendezvous point device, a method comprising:

sending a join request by the host device to the designated device in order to join a shared tree, the join request including an authentication key uniquely associated with the host device;

sending an encoded join request by the designated device to the rendezvous point device, wherein the encoded join request comprises a tag field computed using a keyed hash function and the authentication key ~~and a nonce field comprising a number for preventing playback attack~~;

authenticating the encoded join request by the rendezvous point device by comparing ~~using~~ the host device authentication key against a stored authentication key associated with the host device;

adding the host device to the shared tree, if the encoded join request is authentic; and

excluding the host device from the shared tree, if the encoded join request is not authentic.

66. (canceled)

67. (canceled)

68. (canceled)

69. (canceled)